**Three-factor Authentication (3FA)**

**Knowledge factor**
Something that is known to the user.

**Ownership factor**
Something that the user possesses, like a key or a token.

**Characteristics factor**
A user characteristic, such as biometrics, fingerprints, face scan, voice, etc.

**Knowledge – Type 1 category – something you know**

Password authentication: Secret questions such as mother’s maiden name, favorite food, date of birth, combination/ PIN.

**Characteristics – Type 2 category – something you are**

Biometric authentication: Iris scan, fingerprints, face recognition, voice recognition.

**Ownership – Type 3 category – something you have**

Smart cards or proximity cards simply need to be within proximity to the reader device.

**Levels of Access & Control**

**Centralized administration**
Only one component can control access. Highly centralized control structure.

**Distributed administration**
Access is controlled by information owners. Can be less consistent.

**Audit**
Combination of centralized and decentralized.

**Access Stances**
allow-by-default or deny-by-default

**Authorization**
Access control policies: Level of access and controls granted for a user.

**Access**
Action required to allow information flow between objects.

**Control**
Security measures taken to restrict or allow access to systems.

**Subject**
An entity which requires access to an object or objects.

**Object**
Entity which consists of information.

**Terminology**

**Authentications**

- **Password**
  - Static password: Password does not change. To be avoided.
  - Memory card: A swipe card containing user information.

- **Biometric**
  - Biometric technology allows the user to be authenticated based on physiological or behavioral characteristics.

- **Characteristics**
  - Physiological: Iris, retina, and fingerprints.

- **Ownership factor**
  - Something that the user possesses, like a key or a token.

- **Logical – Type/categorical**
  - Type 1 – something you know
  - Type 2 – something you are
  - Type 3 – something you have

**Authorization Methods**

**Discretionary Access Control (DAC)** - Mandatory Access Control (MAC) - Role-based Access Control (RBAC)

**Access Control Policies**

- **Discretionary**
  - Users are responsible for what actions they have authority to perform.

- **Mandatory**
  - Privileges are assigned to users, but users have no control over their privileges.

- **Role-based**
  - Responsibilities are assigned to roles or groups, and users are assigned to these roles or groups.

**Access Control Requirements**

- **Identity Management**
  - Identification
  - Authorization

- **Security Practices**
  - Quantification of risk

**Federation Models**

- **Identity and Access Management**
  - Federated identity

**Access Control Concepts**

- **Implicit**
  - Access granted to a user as long as they are authenticated.

- **Explicit**
  - Access granted to a user if they meet certain criteria.

**Vulnerability Assessment**

- **Penetration Testing**
  - Testing the security of a system or network.

**Password Types**

- **Simple Passwords**
  - Short, easy to remember.

- **Two-Factor Authentication**
  - Using a second factor for authentication.

**Non-technical Security**

- **Acceptable Use Policy (AUP)**
  - Guidelines for acceptable computer use.

**Penetration Testing**

- **Blind Test**
  - Tests the effectiveness of the organization's security measures.

- **Double-Blind Test**
  - Tests the effectiveness of the organization's security measures without telling the testers who is being tested.

**Password Control Models**

- **Password Policies**
  - Guidelines for password creation and management.

**Policy**

- **Acceptable Use Policy (AUP)**
  - Guidelines for acceptable computer use.

**Task-based access controls**

- **Access Control Policies**
  - Policies that define what actions a user can perform.

- **Access Control Types**
  - Administrative Controls
  - Logical Controls
  - Physical Controls

- **Subject**
  - An entity which requires access to an object or objects.

- **Object**
  - Entity which consists of information.

**Procedure for user account management**

Regular user account review and password change, strict access authorization using a procedure, regularly verify the accounts for active status.